



CDIS Cybercampus Spring Conference 2026



Welcome to CDIS Spring Conference 2026

Musard Balliu, Pontus Johnson, David Olgart
CDIS – Cybercampus Sweden – KTH

SKGgXMc09cc1 lBGDgDg9
aw2z2M0C0m0c1 vEz1101h
Y2hpbm9d9pV2g2F01G21
I2Vz90Gd9pV21tc0V0S8h
bkkg7291e0V0Ym a288sxf1
2NSj284g910000 pcy81NNo
w011000000000000000000
d110000000000000000000
1001100000000000000000
aCb9cy83e00000 u1R0s8s8T
1A0g0Ygc010000 j021w8Kp
bmc9bWj00000 BMLC50a0
WzP0g010000 j021w8K
R1R00000 w1118
M1e00000 110
P1000g



CDIS Cybercampus Spring Conference 2026

Safety First

Emergency exits: 2 on the front and 2 on the back

Entrance doors code: 0642

Gathering point in case of evacuation: Teknikringen 10 A/B





CDIS Cybercampus Spring Conference 2026

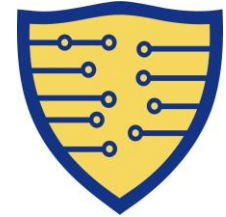


Program:

- 9:00 Welcome and Introduction (Musard Balliu, KTH; Pontus Johnson, KTH; David Olgart, Cybercampus)
- 9:15 Keynote: Formally proved cybersecurity with the seL4 microkernel (June Andronick, Proofcraft)
- 10:00 Team Sweden in the cyber domain (Major General Mattias Hanson, Swedish Armed Forces)
- 10:30 Break
- 11:00 CDIS research and road ahead (Mads Dam, Research coordinator at CDIS, KTH)
- 11:20 CDIS research: Relational reinforcement learning for automated network intrusion response (Jakob Nyberg, CDIS PhD student)
- 11:40 CDIS Alumni: Log4Shell from the inside (Annika Andreasson, PostDoc at HHS)
- 12:00 Lunch; CDIS posters and demos
- 13:30 Defensibility (Ralf Alvarsson and Henrik Karlzén, FOI)
- 13:50 From few to many women in cybersecurity (Agnes Ekman, Martina Dannberg, Linnea Palmqvist)
- 14:10 On the road to ECSC 2028 (Musard Balliu, KTH and Swedish National Hacking Team)
- 14:30 Break
- 15:00 Keynote: Frontier AI for cybersecurity by Mistral AI (August Martens, Mistral AI)
- 15:45 Panel: Digital Sovereignty (Moderator: David Olgart, Cybercampus Sweden). Panelists: June Andronick (Proofcraft), Christian Landgren (Berget), August Martens (Mistral), Magnus Persson (Evroc)
- 16:30 Closing remarks
- 16:40 Reception



CDIS Cybercampus Spring Conference 2026



Poster and Demo Program: 12:00 – 13:30

Tobias Oechtering - Extremal Mechanism for Pointwise Maximal Leakage

Sandor Berglund - Learning to Imitate APTs in Attack Graphs

Vivi Andersson - What makes two CVEs variants?

Henrik Karlsson - Partitioning Kernel with Capability-Controlled Temporal and Spatial Partitioning

Kiarash Kazari - Bayesian Robust Cooperative MARL

Marius Vangeli - Context Relay for Long-Running Penetration-Testing Agents

Sarah Backman - The impact of metaphors on cyber risk perceptions

Syafiq Al Atiiq - Open Source Software Vulnerability Discovery in the Age of AI

Alejandro Russo - When Anonymized Data Isn't Private: How Large Language Models Reveal Emerging Weak Points

Mathias Ekstedt, Joakim Loxdal - Play the TYR game

Anton Israelsson - BOSS: Blinded Oblivious Secret Sampling for Scalable FHE-based MPC



CDIS Cybercampus Spring Conference 2026



Welcome to CDIS Spring Conference 2026

Musard Balliu, Pontus Johnson, David Olgart
CDIS – Cybercampus Sweden – KTH



CYBERCAMPUS SVERIGE

